



Verification of cryptographic protocols: techniques and link to cryptanalysis

Véronique Cortier

► To cite this version:

Véronique Cortier. Verification of cryptographic protocols: techniques and link to cryptanalysis. Sixth International Workshop on Automatic Verification of Critical Systems - AVOCS'06, Sep 2006, Nancy/France. inria-00091656

HAL Id: inria-00091656

<https://inria.hal.science/inria-00091656>

Submitted on 6 Sep 2006

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Verification of cryptographic protocols: techniques and link to cryptanalysis

Véronique Cortier¹

*CNRS — LORIA
Nancy, France*

Abstract

Security protocols are short programs aiming at securing communications over a network. They are widely used in our everyday life. Their verification using symbolic models has shown its interest for detecting attacks and proving security properties. In particular, several automatic tools have been developed. However, the guarantees that the symbolic approach offers have been quite unclear compared to the computational approach that considers issues of complexity and probability. This later approach captures a strong notion of security, guaranteed against all probabilistic polynomial-time attacks.

In this talk, we present several techniques used for symbolically verifying security protocols and we show that it is possible to obtain the best of both worlds: fully automated proofs and strong, clear security guarantees. For example, for the case of protocols that use signatures and asymmetric encryption, we establish that symbolic integrity and secrecy proofs are sound with respect to the computational model against an active adversary.

¹ Email: Veronique.Cortier@loria.fr